

Marked - v/p

Copy

-19-

18.(Four time Amended) A method for protecting software from unauthorised use, by restricting the use thercof to a single person, comprising the steps of:

- a) supplying said software desired to be protected, first software and second software to a processing apparatus ;
- b) [supplying first software and, second software which being specific to a user, to] running said first software on said processing apparatus ;
- c) establishing a communication between said first software running on said processing apparatus, and a remote electronic transaction system ;
- d) verifying said [user] person having a valid account, by said remote electronic transaction system ;
- e) using by said first software, a favourable result of said verification as a pre-condition for determining from said processing apparatus information related to the hardware or/and software thercof, for future reference in step f) below ;

wherein a cost is being charged from said [user] account for the first time said steps a) to e) being carried out ; thereafter

- f) authenticating by said second software, the processing apparatus onwhich said second software is being used, say, second processing apparatus, basing on at least a part of said information related to said hardware or/and software ;
- g) using by said second software, a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on said second processing apparatus, with no charge ;

if the result of said authentication is not favourable, repeat at least said steps c) to e) with said second processing apparatus, without re-charging from said [user] account said cost .

-21-

20(Four time Amended). A method for protecting software, publicly distributed through a communications network, for use by a user, from unauthorised use, comprising the steps of :

a) creating first software ;

wherein "the presence of identity information/means which being specific to [a rightful] said user of said software desired to be protected and being used in enabling operation(s) for which said [rightful] user has to be responsible, in a processing apparatus" is being used in the creation of said first software as a pre-condition for said first software to perform step c) below ;

b) running said first software on said processing apparatus ;

c) determining by said first software running on said processing apparatus meeting said precondition, first information related to the hardware or/and software of said processing apparatus, for future reference in step c) below ;

d) thereafter, determining by second software, from the processing apparatus onwhich said second software is being used, second information related to the hardware or/and software thereof;

e) determining by said second software, if said second information is consistent with said first information ;

f) using by said second software, a favourable result of said determination of consistence as a pre-condition for permitting use of said software desired to be protected on the processing apparatus onwhich said second software is being used ;

repeat at least said step c) with the processing apparatus on which said second software is being used if said result of said determination of consistence is not favourable, without causing any user responsible operation(s) [for which said rightful user has to be responsible,] being performed ;

[wherein said first and second software being specific to said rightful user].

-22-

21(Second Time Amended). A method for verifying identity of a user of a data processing apparatus, comprising the steps of:

- a) receiving, by said data processing apparatus, information specific to a user and necessary for accessing an account of said user ;
- b) verifying said account being valid, by an electronic transaction system, by use of said information received by said data processing apparatus;
- c) using by said data processing apparatus, a favourable result of said verification as a pre-condition for providing user access to at least a part of the functionality of said data processing apparatus ;

wherein said steps a) to c) [is] are being performed without charging said account and said at least a part of functionality being not related to said validity status of said account.

Clear wpy

-19-

18. A method for protecting software from unauthorised use, by restricting the use thereof to a single person, comprising the steps of:

- c) supplying said software desired to be protected, first software and second software to a processing apparatus ;
- d) running said first software on said processing apparatus ;
- e) establishing a communication between said first software running on said processing apparatus, and a remote electronic transaction system ;
- d) verifying said person having a valid account, by said remote electronic transaction system ;
- e) using by said first software, a favourable result of said verification as a pre-condition for determining from said processing apparatus information related to the hardware or/and software thereof, for future reference in step f) below ;

wherein a cost is being charged from said account for the first time said steps a) to e) being carried out ; thereafter

- f) authenticating by said second software, the processing apparatus on which said second software is being used, say, second processing apparatus, basing on at least a part of said information related to said hardware or/and software ;
- g) using by said second software, a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on said second processing apparatus, with no charge ;

if the result of said authentication is not favourable, repeat at least said steps c) to e) with said second processing apparatus, without re-charging from said account said cost .

-21-

20. A method for protecting software, publicly distributed through a communications network, for use by a user, from unauthorised use, comprising the steps of :

[Handwritten signatures: 'J' and 'K' on the left, and 'BEP KJ' on the right]

- a) creating first software ;

whereto "the presence of identity information/means which being specific to said user of said software desired to be protected and being used in enabling operation(s) for which said user has to be responsible, in a processing apparatus" is being used in the creation of said first software as a pre-condition for said first software to perform step

- c) below ;

- b) running said first software on said processing apparatus ;

- c) determining by said first software running on said processing apparatus meeting said precondition, first information related to the hardware or/and software of said processing apparatus, for future reference in step e) below ;

- d) thereafter, determining by second software, from the processing apparatus on which said second software is being used, second information related to the hardware or/and software thereof;

- e) determining by said second software, if said second information is consistent with said first information ;

- g) using by said second software, a favourable result of said determination of consistency as a pre-condition for permitting use of said software desired to be protected on the processing apparatus on which said second software is being used ;

repeat at least said step c) with the processing apparatus on which said second software is being used if said result of said determination of consistency is not favourable, without causing any user responsible operation(s) being performed .

-22-

21. A method for verifying identity of a user of a data processing apparatus, comprising the steps of :

K5
BB
U1

- a) receiving, by said data processing apparatus, information specific to a user and necessary for accessing an account of said user ;
- b) verifying said account being valid, by an electronic transaction system, by use of said information received by said data processing apparatus ;
- c) using by said data processing apparatus, a favourable result of said verification as a pre-condition for providing user access to at least a part of the functionality of said data processing apparatus ;

wherein said steps a) to c) are being performed without charging said account and said at least a part of functionality being not related to said validity status of said account.